

PATENT
Application Serial No. 10/016,078
Docket No. 01-5001

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method for embedding a message within a file, comprising:
 - generating a random key;
 - encrypting the random key to produce an encrypted random key;
 - encrypting the message to produce an encrypted message; and
 - embedding the encrypted random key and the encrypted message in the file, at least one of the encrypted random key and the encrypted message being embedded in random locations throughout the file, wherein the embedding further includes:
 - seeding a random number generator with an intended recipient's public key, and
 - supplementally seeding the random number generator with the random key,
 - embedding the encrypted message at locations in the file corresponding to random numbers generated by the random number generator after supplementally seeding the random number generator with the random key until a total number of bits embedded equals a predetermined percentage of available space within the file, and
 - embedding the encrypted message at sequential unused locations in the file when the total number of bits embedded exceeds the predetermined percentage of available space within the file.

PATENT
Application Serial No. 10/016,078
Docket No. 01-5001

2. (original) The method of claim 1, wherein the generating includes:
generating a random symmetric encryption key.
3. (currently amended) The method of claim 1, wherein the encrypting the random
key includes:
asymmetrically encrypting the random key with [[an]] the intended recipient's public key.
4. (original) The method of claim 2, wherein the encrypting the message includes:
symmetrically encrypting the message with the random symmetric encryption key.
5. (original) The method of claim 1, further comprising:
compressing the message to obtain a compressed message prior to the encrypting the
message.
6. (original) The method of claim 5, further comprising:
encrypting a length of the encrypted message with the random key to obtain an encrypted
message length.
7. (original) The method of claim 6, further comprising:
verifying that the file has sufficient capacity to contain the encrypted message length, the
encrypted random key, and the encrypted message.

PATENT
Application Serial No. 10/016,078
Docket No. 01-5001

8. (original) The method of claim 1, wherein the embedding includes:
randomly embedding both the encrypted random key and the encrypted message
throughout the file
9. (canceled)
10. (currently amended) The method of claim ~~[[9]]~~ 1, wherein the embedding further
includes:
embedding the encrypted random key at locations in the file corresponding to random
numbers generated by the random number generator after the seeding the random number
generator with the intended recipient's public key.
11. (canceled)
12. (currently amended) A method for embedding a message within a file,
comprising:
compressing the message to produce a compressed message;
generating a random key;
encrypting the random key with a public key to produce an encrypted random key;
encrypting the compressed message with the random key to produce an encrypted
message;

PATENT
Application Serial No. 10/016,078
Docket No. 01-5001

encrypting a length of the encrypted message with the random key to produce an encrypted message length;

seeding a random number generator with the public key and supplementally seeding the random number generator with the random key; and

embedding the encrypted random key, the encrypted message length, and the encrypted message in the file, at least one of the encrypted random key, the encrypted message length, and the encrypted message being embedded in locations throughout the file corresponding to random numbers produced by the random number generator;

wherein the embedding further includes:

embedding the encrypted message at locations in the file corresponding to random numbers generated by the random number generator after supplementally seeding the random number generator with the random key until a total number of bits embedded equals a predetermined percentage of available space within the file, and

embedding the encrypted message at sequential unused locations in the file when the total number of bits embedded exceeds the predetermined percentage of available space within the file.

13. (original) The method of claim 12, further comprising:

verifying that the file has sufficient capacity to contain the encrypted message length, the encrypted random key, and the encrypted message.

14. (original) The method of claim 12, wherein the embedding includes:

PATENT
Application Serial No. 10/016,078
Docket No. 01-5001

embedding each of the encrypted random key, the encrypted message length, and the encrypted message in locations throughout the file corresponding to random numbers produced by the random number generator.

15. (canceled)

16. (currently amended) The method of claim [[15]] 12, wherein the supplementally seeding causes the random number generator to produce numbers based on both the random key and a state of the random number generator at a time of the supplementally seeding.

17. (currently amended) The method of claim [[15]] 12, wherein the embedding further includes:

embedding the encrypted random key at locations in the file corresponding to random numbers generated by the random number generator after the seeding the random number generator with the public key.

18. (currently amended) The method of claim [[15]] 12, wherein the embedding further includes:

embedding the encrypted message length at locations in the file corresponding to random numbers generated by the random number generator after the supplementally seeding the random number generator with the random key.

PATENT
Application Serial No. 10/016,078
Docket No. 01-5001

19. (canceled)

20. (canceled)

21. (currently amended) A method for embedding a message within a file, comprising:

- generating a session key;
- encrypting the session key with a public key to produce an encrypted session key;
- encrypting the message with the session key to produce an encrypted message;
- seeding a random number generator with the public key;
- embedding the encrypted session key throughout the file in locations corresponding to random numbers produced by the random number generator;
- seeding the random number generator with the session key;

and

- embedding the encrypted message throughout the file in locations corresponding to random numbers produced by the random number generator after the seeding with the session key wherein the embedding includes:
 - embedding the encrypted message at locations in the file corresponding to random numbers generated by the random number generator after seeding the random number generator with the session key until a total number of bits embedded in the file equals a determined percentage of available space within the file, and

PATENT
Application Serial No. 10/016,078
Docket No. 01-5001

embedding the encrypted message at sequential unused locations in the file when the total number of bits embedded exceeds the determined percentage of available space within the file.

22. (original) The method of claim 21, further comprising:
encrypting a length of the encrypted message with the session key to produce an encrypted message length; and
embedding the encrypted message length throughout the file in locations corresponding to random numbers produced by the random number generator after the seeding with the session key.

23. (canceled)

24. (canceled)

25. (currently amended) The method of claim ~~[[23]]~~ 21, wherein the determined percentage is a fixed percentage.

26. (currently amended) The method of claim ~~[[23]]~~ 21, further comprising:
randomly determining the determined percentage.

PATENT
Application Serial No. 10/016,078
Docket No. 01-5001

27. (currently amended) A computer-readable medium that stores instructions executable by one or more processors to embed a message within a file, comprising:

- instructions for generating a random session key;
- instructions for encrypting the session key to produce an encrypted session key;
- instructions for encrypting the message to produce an encrypted message;
- instructions for seeding a random number generator;
- instructions for randomly embedding the encrypted session key throughout the file in locations corresponding to random numbers produced by the random number generator;
- instructions for re-seeding the random number generator;

and

- instructions for embedding the encrypted message throughout the file in locations corresponding to random numbers produced by the random number generator after the re-seeding, the embedding continuing until a total number of bits embedded in the file equals a determined percentage of available space within the file; and
- instructions for randomly determining the determined percentage.

28. (currently amended) A processing device, comprising:

- a processor; and
- a memory operatively coupled to the processor and containing a message, a file, and instructions which when executed by the processor perform the functions of:
 - generating a random key,
 - encrypting the random key to produce an encrypted random key,

PATENT
Application Serial No. 10/016,078
Docket No. 01-5001

encrypting the message to produce an encrypted message, and
embedding the encrypted random key and the encrypted message in the file, at
least one the encrypted random key and the encrypted message being embedded in random
locations throughout the file, wherein the embedding further includes:

seeding a random number generator with an intended recipient's public
key, and supplementally seeding the random number generator with the random key,

embedding the encrypted message at locations in the file corresponding to
random numbers generated by the random number generator after supplementally seeding the
random number generator with the random key until a total number of bits embedded equals a
predetermined percentage of available space within the file, and

embedding the encrypted message at sequential unused locations in the file
when the total number of bits embedded exceeds the predetermined percentage of available space
within the file.

29. (new) A method for embedding a message within a file, comprising:
- generating a session key;
 - encrypting the session key with a public key to produce an encrypted session key;
 - encrypting the message with the session key to produce an encrypted message;
 - seeding a random number generator with the public key;
 - embedding the encrypted session key throughout the file in locations corresponding to
random numbers produced by the random number generator;
 - seeding the random number generator with the session key;

PATENT
Application Serial No. 10/016,078
Docket No. 01-5001

embedding the encrypted message at locations in the file corresponding to random numbers generated by the random number generator after seeding the random number generator with the session key, the embedding continuing until a total number of bits embedded in the file equals a determined percentage of available space within the file; and
randomly determining the determined percentage.